The FBI Won't Say Whether It Hacked Dark Web ISIS Site

Joseph Cox ⋮ 5-6 minutes

Image: Ahmad Al-Rubaye/Staff

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

U.S. government lawyers are hampering efforts that could reveal how the FBI managed to obtain the real IP address of an alleged visitor to an ISIS website on the dark web, according to court records reviewed by Motherboard.

The case involves Muhammed Momtaz Al-Azhari, who was charged in May 2020 with attempting to provide material support to ISIS. According to the complaint against him, Al-Azhari allegedly visited a dark web site that hosts “unofficial propaganda and photographs related to ISIS” multiple times on May 14, 2019. In virtue of being a dark web site—that is, one hosted on the Tor anonymity network—it should have been difficult for the site owner’s or a third party to determine the real IP address of any of the site’s visitors.

> ***Do you know anything else about the FBI’s use of NITs? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, or email joseph.cox@vice.com.***

Yet, that’s exactly what the FBI did. It found Al-Azhari allegedly visited the site from an IP address associated with Al-Azhari’s grandmother’s house in Riverside, California. The FBI also found what specific pages Al-Azhari visited, including a section on donating Bitcoin; another focused on military operations conducted by ISIS fighters in Iraq, Syria, and Nigeria; and another page that provided links to material from ISIS’s media arm. Without the FBI deploying some form of surveillance technique, or Al-Azhari using another method to visit the site which exposed their IP address, this should not have been possible.

Now, in a recent series of filings, Department of Justice lawyers won't say how the agency accessed Al-Azhari's IP address, and are blocking discussion of the issue from entering the public docket.

“In discovery, the Government has declined to provide any information related to its TOR operation,” Samuel E. Landes, the defense attorney working on the case, wrote in a filing published Tuesday.

The news highlights the Department of Justice's continued and intense secrecy about its use of hacking tools, despite them becoming more popular in a wide range of types of criminal investigations. The knock-on effects of that secrecy can be that defendants do not have access to details of how they were identified, and don’t have an opportunity to effectively challenge its legal basis. In some cases, prosecutors have also lost chances of convictions because keeping the tools secret was deemed more important than winning a case.

In the motion filed Tuesday, Landes writes that government prosecutors have successfully demanded his motion to compel for more information be marked as a “highly sensitive document.” That designation is used for documents that may be of interest to the intelligence service of a hostile foreign government, and use of which by the foreign government would likely cause significant harm, Landes filing says. Landes’ latest filing is a subsequent motion asking the court to reconsider giving that designation to his earlier motion.

Landes points to how the FBI’s use of network investigative techniques (NITS)—the DOJ’s euphemism for hacking tools—is far from a secret, having been used in multiple cases over the years. He says he also found an exhibit filed in other cases with similar issues and is widely available

on the internet. Despite the public availability of this information, the government asked the court to treat the motion to compel as a highly sensitive document, Landes writes.

The Department of Justice declined to comment.

In other cases, the DOJ has decided to stop pursuing convictions altogether rather than provide defendants with more information on how they were identified. In 2015 the FBI took over, and hacked thousands of visitors to, a dark web child abuse site. While the operation did ultimately secure many convictions, prosecutors refused to abide by an order from the court to provide the defense team with the NIT exploit code. The judge threw out the evidence in response, killing the case. The NIT was based on a "non-public" vulnerability.